ELSEVIER

Journal of Pure and Applied Algebra 163 (2001) 193–207

JOURNAL OF PURE AND APPLIED ALGEBRA

www.elsevier.com/locate/jpaa

Monogenic bialgebras over finite fields and rings of Witt vectors

Alan Koch

Department of Mathematics, Agnes Scott College, Decatur, GA 30030, USA

Received 2 March 1999; received in revised form 19 July 2000
Communicated by F. Oort

Abstract

We classify a certain collection of bialgebras that are generated by a single element over a finite field k, giving a parameterization using positive integers. We then put necessary and sufficient conditions on this pair so that the bialgebra lifts uniquely to the ring $W(k)$ of Witt vectors with coefficients in k, and finally provide a formula for the number of such lifts. © 2001 Elsevier Science B.V. All rights reserved.

MSC: Primary: 16W30; secondary: 14L15, 13K05

The purpose of this paper is to prove the following three theorems:

Theorem 1. *Monogenic local–local cocommutative involutive bialgebras over the finite field $k = \mathbf{F}_{p^\ell}$ are in one-to-one correspondence with the set*

$$\mathbf{Z}^+ \cup \{(n,r,z) \mid n \geq 1, r \leqslant n-1, 0 \leq z \leq p^d - 2, d = \gcd(\ell, r+1)\}.$$

Theorem 2. *The monogenic local–local cocommutative involutive bialgebra corresponding to (n,r,z) lifts to an unramified extension of $\mathbf{Z}_p$ if and only if $r+1$ divides n. Furthermore, any monogenic local–local cocommutative bialgebra that corresponds to an element of $\mathbf{Z}^+$ does not lift.*

Theorem 3. *If $n = s(r+1)$, then the number isomorphism classes of $\mathbf{Z}_{p^\ell}$-bialgebras H such that is a lift of the monogenic local–local cocommutative involutive $\mathbf{F}_{p^\ell}$-bialgebra*

E-mail address: akoch@agnesscott.edu (A. Koch).

PII: S0022-4049(00)00163-8

corresponding to (n,r,z) *is*

$$p^{\ell r(s-1)+d(s-1-f(z))},$$

where $d=\gcd(\ell,r+1)$, $f(z)=\#\{i \mid 1 \le i \le n-r-1, (p^d-1)|(z(p^i-1))\}$. *In particular, there is only one isomorphism class if and only if* $s=1$ *or we have both* $k \subseteq \mathbf{F}_{p^{r+1}}$ *and* $(p^\ell-1)/(p^d-1)$ *divides* z.

Following the terminology of [1] (where the term *Hopf algebra* is used in place of involutive bialgebra), a bialgebra is said to be *monogenic* if it is generated as an algebra by a single element. In addition, we shall say a bialgebra H is *local–local* if both H and its linear dual H^* are local rings. We assume throughout this paper that all bialgebras are involutive, i.e. there exists an antipodal map $\lambda : H \to H$.

Let k be a finite field of characteristic p. The proofs of the above theorems use Dieudonné modules. Dieudonné modules can be used to describe finite connected unipotent commutative group schemes over perfect fields k of characteristic p (as well as more general group schemes and formal groups which will not be discussed here). Such group schemes correspond to finite local–local cocommutative k-bialgebras, so we can use Dieudonné modules to give the parameterization in Theorem 1. We shall see that the monogenic bialgebras give rise to a specific subclass of Dieudonné modules whose structure is fairly easy to describe. It is known that a monogenic local–local bialgebra can be expressed in the form $k[t]/(t^{p^n})$ for some n [10, p. 112], so the problem is to determine the number of possible comultiplications up to isomorphism. We will see that each comultiplication can be parameterized by either a positive integer or a triple of positive integers satisfying certain conditions. This will prove the first theorem.

For H a k-bialgebra and R a characteristic zero discrete valuation ring with residue field k, we say that H *lifts* to R if there is a finite free R-bialgebra H_R so that $H_R \otimes_R k \cong H$. All bialgebras lift to some such R [7, Corollary 5.1], however it is not the case that every bialgebra lifts to every R – one example being the unique local–local bialgebra of dimension p over $\mathbf{F}_p$, which does not lift to $\mathbf{Z}_p$ [9, p. 21]. In this particular example, the problem arises in that there is not enough ramification in $\mathbf{Z}_p$. When we replace R by a ramified extension of $\mathbf{Z}_p$, we get a lift. The presence of ramification appears to facilitate lifting in some cases (see, e.g., [1,9]). In fact, in [8, p. 69, Corollary 2] it is shown that when $1 < e \le p-1$, $p \ge 5$, any bialgebra lifts.

For this reason we shall turn our attention only to unramified extensions of $\mathbf{Z}_p$. These rings arise as rings of Witt vectors for some perfect field k of characteristic $p > 0$. The lifting questions, existence and uniqueness, will be handled using finite Honda systems. Honda developed a method of describing lifts of formal groups to $W(k)$, which was later adapted by Fontaine for finite group schemes. A finite Honda system consists of a Dieudonné module (corresponding to the original group scheme) and a $W(k)$-submodule satisfying certain properties. Using this criterion along with the particularly simple Dieudonné module structure for our bialgebras, we are able to quickly determine precisely when we can lift to $W(k)$, and also when this lift is unique. Finally, we provide a formula for the number of lifts (in the sense described

above) for a given k-bialgebra. The size of the bialgebra, the size of the field, and the particular choice of z play a major role in this formula.

It is a consequence of Nakayama's Lemma that any monogenic k-bialgebra that lifts does so to a monogenic $W(k)$-bialgebra. Thus, one way of studying monogenic $W(k)$-bialgebras is to find all of the monogenic k-bialgebras and their lifts to $W(k)$. The results of this paper should give insight on classifying monogenic bialgebras over $W(k)$ for the case when the k-bialgebra (obtained by reduction modulo p) is local–local.

In addition to having an antipode, we shall assume throughout that all bialgebras are finite-dimensional (as modules), commutative, and local–local.

1. Dieudonné modules and bialgebras

Let k be a perfect field of characteristic p. (Later, we will restrict ourselves to the case when k is finite.) We shall start by describing the correspondence between Dieudonné modules and k-bialgebras. Let $W = W(k)$ be the ring of Witt vectors with coefficients in k. Recall that W is the collection of infinite-length vectors whose ring operations are given by certain polynomials: S_n gives the nth vector component for the sum, and P_n gives the nth vector component for the product (where the components are numbered starting with 0). These polynomials can be found in [4, p. 128]. The ring $W(k)$ is a discrete valuation ring with maximal ideal (p) and residue field k.

Let E be the noncommutative ring of polynomials $E = W[F, V]$ with the relations $FV = VF = p, Fw = w^\sigma F, wV = Vw^\sigma$, where $w \in W$ and w^σ is simply w with each component raised to the pth power. (We shall adopt a similar notation for elements of E: e^σ refers to applying $(\ )^\sigma$ to the W-coefficients of e.) Note that if $k = \mathbf{F}_p$, then $W(k) = \mathbf{Z}_p$ and E is actually commutative since $w^\sigma = w$. The term *Dieudonné module* refers to a left E-module M that is killed by both a power of F and a power of V.

Of particular interest to us will be Dieudonné modules that are cyclic, i.e. that are of the form E/I where I is a left ideal of E. An easy but useful result concerning cyclic Dieudonné modules is

Lemma 1.1. *Let M be a cyclic Dieudonné module and let x be a generator of M. For any $e \in E$, $(1 - eF)x$ is an invertible element of M, i.e. there exist $e_1, e_2 \in E$ so that $e_1(1 - eF)x = (1 - eF)e_2x = x$.*

Proof. As M is a Dieudonné module, it is killed by some power of F, say F^n. Let $e_1 = ((1 + e^\sigma F + e^{\sigma^2}F + \cdots + e^{\sigma^{n-1}}F^{n-1})x)$ and $e_2 = ((1 + eF + ee^\sigma F^2 + c \cdots + ee^\sigma e^{\sigma^2} \cdots e^{\sigma^{n-1}}F^{n-1})x)$. Then it is a routine exercise to verify that

$$e_1((1 - eF)x) = ((1 - eF)x)e_2 = (1 + e'F^n)x$$

for some $e' \in E$. Since $F^n x = 0$, we have constructed left and right inverses for $(1 - eF)x$. □

As an important consequence to this lemma, if $(1-eF)m=0$ for $m\in M$, then $m=0$: multiplying by the e_1 above gives $e_1(1-eF)m=(1+e'F^n)m=m$.

To any Dieudonné module M be can associate a k-bialgebra $\mathscr{H}(M)$ in the following way. As a k-algebra, $\mathscr{H}(M)=k[T_x\,|\,x\in M]$ with the following relations:

$$T_{F_x}=(T_x)^p,$$

$$T_{x+y}=S_N((T_{V^Nx},T_{V^{N-1}x},\ldots,T_x);(T_{V^Ny},T_{V^{N-1}y},\ldots,T_y)),$$

$$T_{wx}=P_N((w_0^{p^{-N}},w_1^{p^{-N}},\ldots,w_N^{p^{-N}});(T_{V^Nx},T_{V^{N-1}x},\ldots,T_x)),$$

where $x,y\in M$, $w=(w_0,w_1,\ldots)\in W(k)$, and N is any nonnegative integer so that $V^{N+1}M=0$. The comultiplication is given by

$$\Delta(T_x)=S_N((T_{V^Nx}\otimes 1,T_{V^{N-1}x}\otimes 1,\ldots,T_x\otimes 1);(1\otimes T_{V^Nx},1\otimes T_{V^{N-1}x},\ldots,1\otimes T_x)).$$

These operations make $\mathscr{H}(M)$ into a (local–local) bialgebra. In fact, this gives a 1–1 correspondence between finite local–local cocommutative bialgebras and Dieudonné modules. See [3, II, Section 5] for a complete description of this correspondence (explained in terms of the group scheme $\mathrm{Spec}(H)$ rather than H). The size of the bialgebra and the size of the Dieudonné module are related by

$$\mathrm{rank}_k\mathscr{H}(M)=p^{\mathrm{length}_{W(k)}M}.$$

We shall refer to this fact several times in the next section.

2. Monogenic bialgebras in characteristic p

Lemma 2.1. *Let M be a Dieudonné module. Then $\mathscr{H}(M)$ is a monogenic bialgebra if and only if M is cyclic and there exists a polynomial $q(F)\in k[F]$ such that for all $x\in M$ we have $Vx=q(F)x$.*

Proof. Suppose M is cyclic and $Vx=q(F)x$ for all $x\in M$. Take $x=1_M$, i.e. x is the element corresponding to 1 under the canonical map $E\to M\cong E/I$. Then $px=Fq(F)x$, so M has a k-basis consisting of $\{x,Fx,F^2x,\ldots,F^{n-1}x\}$ for some n. We claim that $F^nx=0$. Suppose

$$F^nx=\sum_{i=\ell}^{n-1}a_iF^ix,\quad a_\ell\neq 0.$$

Then

$$\begin{aligned}-a_\ell F^\ell x&=a_{\ell+1}F^{\ell+1}x+a_{\ell+2}F^{\ell+2}x+\cdots+a_{n-1}F^{n-1}x-F^nx\\&=(a_{\ell+1}Fx+a_{\ell+2}F^2x+\cdots+a_{n-1}F^{n-1-\ell}x-F^{n-\ell}x)F^\ell x.\end{aligned}$$

Moving all of the terms to the left and multiplying by $-a_\ell^{-1}$ gives $(1-eF)F^\ell x=0$, where $e=-a_\ell^{-1}a_{\ell+1}-a_\ell^{-1}a_{\ell+2}F-\cdots-a_\ell^{-1}a_{n-1}F^{n-2-\ell}-a_\ell^{-1}F^{n-\ell-1}$. But $(1-eF)x$ is invertible in M, so we have $F^\ell x=0$, i.e. $F^\ell M=0$, which is impossible. Thus $F^nx=0$.

Notice that there is a chain of $W(k)$-modules

$$0 = F^n M \subseteq F^{n-1} M \subseteq F^{n-2} M \subseteq \cdots \subseteq FM \subseteq M.$$

We claim that for $0 \leq i \leq n-1$ we have $F^{i+1}M \subset F^i M$, i.e. that we have a strict containment of sets. Clearly we have $F^{i+1}M \subseteq F^i M$. If the two sets are in fact equal, then there exists an $e \in E$ so that $eF^{i+1}x = F^i x$. This would give

$$F^i x = eF^i(Fx)$$

or in other words

$$(1 - eF)F^i x = 0.$$

But again $(1-eF)x$ is invertible in M, hence $F^i x = 0$ which is a contradiction, proving our claim. Clearly, this is also a minimal chain, so the length of M is n.

Let t be the element in $\mathscr{H}(M)$ corresponding to x, i.e. $t = T_x$. Then $T_{F^i x} = t^{p^i}$, so $t^{p^n} = 0$ and $t^{p^{n-1}} \neq 0$. Thus, T_x generates the k-algebra $H = k[t]/(t^{p^n})$, which is a bialgebra of dimension p^n. As $\operatorname{rank}_k \mathscr{H}(M) = p^n = p^{\operatorname{length}_{W(k)} M}$ it follows that $\mathscr{H}(M) \cong H = k[t]/(t^{p^n})$.

Conversely, let $\mathscr{H}(M) \cong k[t]/(t^{p^n})$. Again we have $\operatorname{rank}_k \mathscr{H}(M) = p^n = p^{\operatorname{length}_{W(k)} M}$, so M has length n. Let x be an element in M corresponding to $t \in \mathscr{H}(M)$. Then $F^n x = 0$ and $F^{n-1} x \neq 0$. Let $M' \subseteq M$ be the E-submodule of M generated by x. By an argument similar to the one above, it is clear that $F^{i+1}M' \subset F^i M'$. Thus we have a chain of $W(k)$-modules

$$0 = F^n M' \subset F^{n-1} M' \subset F^{n-2} M' \subset \cdots \subset FM' \subset M' \subseteq M$$

which has length $n+1$, hence $M' = M$ and M is cyclic.

It remains to show that $Vx = q(F)x$ for some polynomial $q(F) \in k[F]$. Consider the chain of $W(k)$-modules

$$0 = F^n M \subset F^{n-1} M \subset F^{n-2} M \subset \cdots \subset FM \subseteq FM + VM \subseteq M.$$

As the length of this chain is $n+1$ we have either $FM + VM = FM$ (in which case $VM \subseteq FM$) or $FM + VM = M$. If $FM + VM = M$, then we can write the generator x as $x = Fex + Ve'x$. Let N be the smallest positive integer for which $V^{N+1} M = 0$. Then $V^N x = V^N Fex + V^{N+1} e'x = V^N Fex \neq 0$, so $(1 - e^{\sigma^{-N+1}} F)V^N x = 0$, hence $V^N x = 0$, which is a contradiction. Thus $VM \subseteq FM$.

We therefore have $Vx = Fex$ for some e. We separate the "strictly F" part of e by writing $e = a(F) + e'V$, $a(F) \in k[F]$. Then

$$\begin{aligned} Vx &= F(a(F) + e'V)x \\ &= a(F)^\sigma Fx + e'^\sigma FVx \\ &= a(F)^\sigma Fx + e'^\sigma F(a(F) + e'V)x = \cdots \\ \cdots &= a_1(F)Fx + a_2(F)F^2 x + \cdots + a_{n-1}(F)F^{n-1}x + e_0 VF^n x \end{aligned}$$

for some choice of polynomials $a_1(F),\ a_2(F),\ldots,a_n(F)\in k[F]$ and $e_0\in E$. Since $F^n x=0$, we see that Vx can be expressed as a polynomial in $k[F]$, a polynomial which we shall denote by $q(F)$. □

Proposition 2.2. *Let $\mathscr{H}(M)$ be a monogenic bialgebra. Then*

$$M\cong E/E(F^n,F^r-\eta V)$$

for $\eta\in k^\times$ and for some pair of integers (n,r) with $1\le r\le n$.

Proof. Since M is cyclic $M/pM\cong E/E(F^{r+1},F^r-\eta V)$ or $M/pM\cong E/E(F^n,V)$ [6, Theorem 2.1]. Let $x=1_M$. Since $Vx=q(F)x$, we have $M\cong E/(E(q(F)-V)+pI)$ for some ideal $I\subseteq E$ and $q(F)\equiv\eta^{-1}F^r(\mathrm{mod}\ p)$. Let n be the smallest integer so that $F^nM=0$. Then $F^n\in(q(F)-V)+pI$, i.e. $F^n=e_1(q(F)-V)+e_2p$ for some $e_1,e_2\in E$. Thus

$$e_1q(F)=F^n-(e_2F-e_1)V.$$

Writing $e_1=a(F)+eV,\ a(F)\in k[F]$ on the left-hand side we get

$$a(F)q(F)+Vq(F)=F^n-(e_2F-e_1)V.$$

As the powers of V are linearly independent in E, we have $a(F)q(F)=F^n$, so $q(F)=cF^i$ for some $c\in k$ and some $0\le i\le n$. Clearly $i\neq 0$, as this would give $Vx=F^0x=x$, which would contradict the fact that M is killed by a power of V. Hence $1\le i\le n$. As $q(F)\equiv\eta^{-1}F^r(\mathrm{mod}\ p)$, we can set $c=\eta^{-1}$ and obtain $q(F)=\eta^{-1}F^r$, so $M\cong E/(E(F^r-\eta V)+pI)$. Since $F^nM=0$, we can rewrite this as $M\cong E/(E(F^n,F^r-V)+pI)$.

We now claim that $pI\subseteq(F^n,F^r-\eta V)$, which will finish this proof. Since $Vx=\eta^{-1}F^rx$, we can regard elements in pI as polynomials in $k[F]F^{r+1}$. Let $g(F)\in pI$, $g(F)=cF^\ell-h(F)F^{\ell+1}$ with $c\neq 0,\ \ell\ge r+1$. By multiplying throughout by c^{-1} we can take $c=1$. Then, since $g(F)x=0$ we have

$$F^\ell x=h(F)F^{\ell+1}x=(h(F)F)F^\ell x$$

so $(1-h(F)F)F^\ell x=0$. By Lemma 1.1, $F^\ell x=0$, so $\ell\ge n$, i.e. $g(F)\in(F^n,F^r-\eta V)$. Thus $M\cong E/E(F^n,F^r-\eta V)$. □

Note that in the case $r=n$ the module simplifies to $E/E(F^n,V)$.

3. The isomorphism classes of monogenic bialgebras

While this describes all monogenic bialgebras, the description is not a unique one. However, it is clear that all of the Dieudonné modules of the form $E/E(F^n,V)$ are mutually nonisomorphic: the power of F that kills M is invariant under isomorphism. It is also not hard to show that $E/E(F^n,V)$ is not isomorphic to $E/E(F^n,F^r-\eta V)$ for any $r<n$. However, it is possible for two bialgebras corresponding to triples to

be isomorphic, although the bialgebra corresponding to the triple (n_1, r_1, η_1) is not isomorphic to the bialgebra given by (n_2, r_2, η_2) unless $n_1 = n_2$ and $r_1 = r_2$. For the remainder of the paper we assume k is finite and write $k = \mathbf{F}_{p^\ell}$. We shall now determine when two such bialgebras are isomorphic over k.

Suppose $M_1 = E/E(F^n, F^r - \eta_1 V)$ and $M_2 = E/E(F^n, F^r - \eta_2 V)$. An isomorphism of bialgebras corresponds to an E-module isomorphism $\varphi : M_1 \to M_2$. If we let $x = 1_{M_1}$ and $y = 1_{M_2}$, then there exists a polynomial $u(F) \in k[F]$ with nonzero constant term such that $\varphi(x) = u(F)y$. In order to be an E-module map, we have $\varphi(F^r x) = \varphi(\eta_1 V x)$, i.e. $F^r u(F)y = \eta_1 V u(F)y$.

Write $u(F)y = \sum_{i=0}^{n-1} u_i F^i y$. Then

$$F^r u(F)y = \sum_{i=0}^{n-1} F^r u_i F^i y = \sum_{i=0}^{n-1} u_i^{p^r} F^{r+i} y$$

and

$$\eta_1 V u(F)y = \sum_{i=0}^{n-1} \eta_1 V u_i F^i y = \sum_{i=0}^{n-1} \eta_1 u_i^{p^{-1}} F^i V y$$

$$= \sum_{i=0}^{n-1} \eta_1 u_i^{p^{-1}} F^i \eta_2^{-1} F^r y = \sum_{i=0}^{n-r-1} \eta_1 \eta_2^{-p^i} u_i^{p^{-1}} F^{r+i} y.$$

By comparing coefficients, it follows that $u_i^{p^r} = \eta_1 \eta_2^{-p^i} u_i^{p^{-1}}$ for all i less than $n - r$. Satisfying this condition is quite simple for $i \neq 0$: simply take $u_i = 0$. However, to be an isomorphism, $u_0 \neq 0$. We can rewrite the condition and say

$$\left(\frac{\eta_1}{\eta_2^p}\right) = u_0^{p^r - p^{-1}}.$$

This equation was examined in [6, Theorem 3.8] to determine isomorphism classes of cyclic Dieudonné modules killed by p, where it was shown that solutions of this equation over $\mathbf{F}_{p^\ell}$ are in one-to-one correspondence with elements of the quotient group $k^\times / k_0^\times$, where $k_0 = \mathbf{F}_{p^d}$, $d = \gcd(\ell, r+1)$. Thus the number of isomorphism classes is $|k^\times| / (|k^\times| / |k_0^\times|) = |k_0^\times| = p^d - 1$. In fact, if we pick $\alpha \in k$ so that $k = k_0[\alpha]$, then $\eta_1 = \alpha^{i_1}$ and $\eta_2 = \alpha^{i_2}$, and it was easy to determine when their bialgebras are isomorphic.

Proposition 3.1. *Let k, k_0 be as above. All cyclic Dieudonné modules corresponding to monogenic bialgebras are either of the form $E/E(F^n, V)$ or $E/E(F^n, F^r - \alpha^z V)$ with $1 \leq r \leq n-1$, $0 \leq z \leq p^d - 2$, $d = \gcd(\ell, r+1)$.*

Theorem 1 immediately follows from this proposition. In addition, since there are $p^d - 1$ different choices for z, this result enables us to give a formula for the exact number of monogenic bialgebras of a given size.

Corollary 3.2. *The number of isomorphism classes of monogenic bialgebras over* $k = \mathbf{F}_{p^\ell}$ *of dimension* p^n *is given by*

$$1 + \sum_{r=1}^{n-1} (p^{\gcd(\ell, r+1)} - 1).$$

4. Finite Honda systems and lifts of monogenic bialgebras

Now that the classification of monogenic bialgebras over k is complete, we shall turn our attention to monogenic bialgebras over the ring of Witt vectors $W(k)$. We shall briefly describe the method for lifting k-bialgebras to $W(k)$ using finite Honda systems. Such a system is a finite analogue to Honda's method for classifying p-divisible groups over $W(k)$. (Further details can be found in [2].) We then apply those results to our Dieudonné modules, and find that lifting depends on a very simple relationship between n and r.

Definition 4.1. A finite Honda system over $W(k)$ is a pair (M, L), where M is a Dieudonné module (over k) and L is a $W(k)$-submodule of M such that

(i) $\ker V \cap L = 0$;
(ii) The canonical map $L/pL \to M/pM \to \operatorname{coker} F$ is an isomorphism.

We shall usually identify L/pL with its image in $\operatorname{coker} F$ and rewrite the second condition as $L/pL = M/FM$.

Given two finite Honda systems (M, L) and (M', L'), we define a morphism $(M, L) \to (M', L')$ to be an E-module homomorphism $\varphi : M \to M'$ with the extra condition that $\varphi(L) \subseteq L'$. If E is in fact an isomorphism, then we say that the finite Honda systems (M, L) and (M', L') are isomorphic. The objects (M, L) together with the morphisms form a category, typically denoted $FH(W(k), k)$.

Given any Dieudonné module M, the finite Honda systems (M, L) that we can construct correspond to lifts of $\mathscr{H}(M)$ to $W(k)$. In fact, there is a one-to-one correspondence between the lifts of $\mathscr{H}(M)$ and isomorphism classes of finite Honda systems (M, L) for various L, and this correspondence takes morphism to morphisms, making it an equivalence of categories. The actual correspondence is quite complicated, but it can be found it [2, pp. 1424–1425], where the results are written in the language of group schemes rather than bialgebras.

We shall now determine precisely when a monogenic k-bialgebra lifts to $W(k)$. One way of determining the existence of a lift can be found in [5, Theorem 4.1]; however, here we will be able to describe all lifts when the bialgebras are monogenic. If $H = \mathscr{H}(M)$, $M = E/E(F^n, F^r - \alpha^z V)$, the question is reduced to finding an L so that (M, L) is a finite Honda system. We can quickly see that the case where $n = r$, i.e. $M = E/E(F^n, V)$, does not lift: there are no finite Honda systems (M, L) for this M since any $L \subseteq M = \ker V$. Thus it would appear that there needs to be some relationship between the n and the r. This relationship is found in the following:

Proposition 4.2. *Let $M = E/E(F^n, F^r - \alpha^z V)$. Then $\mathscr{H}(M)$ lifts to $W(k)$ if and only if $r+1$ divides n.*

Proof. Let $x = 1_M$. Under the canonical isomorphism we have $M/FM = E/E(F^n, V)$, so we can pick any single element of $m \in M$ to generate $\operatorname{coker} F$ provided $m \notin FM$. Thus, we need to find a $W(k)$-submodule $L \subseteq M$ so that L is generated by a single nontrivial element $(\operatorname{mod} FM)$ over k and $L \cap \ker V = 0$, or show that there is no such L.

Suppose first that $n = s(r+1)$. Not only shall we find a suitable L, we will find all L for which (M, L) is a finite Honda system. For notational convenience, set $\eta = \alpha^z$, and define $\eta_t = \prod_{i=0}^{t} \eta^{p^{i(r+1)}}$. Let $g(F)$ be any invertible element in the noncommutative ring $k[F]/(F^n)$. (It is easy to check that the group of invertible elements, denoted $(k[F]/(F^n))^\times$, consists of all polynomials with a nonzero constant term.) Define L_g to be the $W(k)$-submodule of M generated by the single element $g(F)$. Clearly $g(F) \notin FM$.

We claim in addition that $\ker V \cap L_g = 0$. Notice that $p^s M = F^n M = 0$. Thus, any $w \in W(k)$ acting nontrivially can be replaced by the finite sum $w = \sum_{i=t}^{s-1} w_i p^i$, $w_i \in k$, $w_t \neq 0$. For any such w, we need to show that $V(wg(F)) \neq 0$. Write $g(F) = g_0 + g'(F)F$, $g_0 \neq 0$ and $w = w_t p^t + w' p^{t+1}$. Then

$$wg(F)x = (w_t p^t + w' p^{t+1})(g_0 + g'(F)F)x = w_t g_0 p^t x + w' g_0 p^{t+1} x + eF p^t x$$

for some $e \in E$. Since $px = \eta^{-1} F^{r+1} x$ we have $p^t x = \eta_t^{-1} F^{t(r+1)} x$ and hence

$$\begin{aligned} V(wg(F)x) &= V(\eta_t^{-1} w_t g_0 F^{t(r+1)} x + \eta_{t+1}^{-1} w' g_0 F^{(t+1)(r+1)} x + e\eta_t^{-1} F^{t(r+1)+1} x) \\ &= (\eta_t^{-1} w_t g_0)^{p^{-1}} F^{t(r+1)+r} x + (\eta_{t+1}^{-1} w' g_0)^{p^{-1}} F^{(t+1)(r+1)} x \\ &\quad + e^{\sigma^{-1}} \eta_t^{-1} F^{(t+1)(r+1)} x \\ &\equiv (\eta_t^{-1} w_t g_0)^{p^{-1}} F^{t(r+1)+r} x (\operatorname{mod} F^{(t+1)(r+1)}). \end{aligned}$$

But $t(r+1) + r \leq (s-1)(r+1) + r = s(r+1) - 1 = n - 1$, and since $(\eta_t w_t g_0)^{p^{-1}} \neq 0$ it follows that $V(wg(F)x) \neq 0$. Thus (M, L_g) is a finite Honda system, so L_g provides a lift.

Conversely, suppose $r+1$ does not divide n. Let L be a $W(k)$-submodule of M such that $L/pL = M/FM$. We shall show that $\ker V \cap L \neq 0$. Since $L/pL = M/FM$, there exists some element of the form $x + Fex \in L$ to correspond to the element $x = 1_M$. Let i be the unique integer so that

$$\frac{n-r}{r+1} \leq i \leq \frac{n-1}{r+1}.$$

We know that such an i exists: clearly the set

$$\left\{ \frac{n-r}{r+1}, \frac{n-2}{r+1}, \ldots, \frac{n-(r+1)}{r+1} \right\}$$

contains exactly one integer, and since $r+1$ does not divide n, we can eliminate the last member of this set. Thus i is the unique integer such that $n-r \le i(r+1) \le n-1$.

We have $p^i(x+Fex) \in L$. But

$$p^i(x+Fex) = (1+Fe)p^i x = (1+Fe)\eta_i^{-1}F^{i(r+1)}x$$

which is nonzero as $i(r+1) < n$. Thus, it follows that

$$V(p^i(x+Fex)) \equiv \eta_i^{-1}F^{i(r+1)+r}x \,(\mathrm{mod}\, F^{(i+1)(r+1)}).$$

But $i(r+1) \ge n-r$, so $V(p^i(e_1x+Fe_2x)) = 0$, hence $p^i(e_1x+Fe_2x) \in \ker V$. □

5. Questions concerning the uniqueness of lifts

We will eventually obtain a formula for the total number of isomorphism classes of lifts a monogenic bialgebra has to $W(k)$. But for now, we address the question: when does a k-bialgebra lift *uniquely* to $W(k)$? In other words, when is there precisely one isomorphism class of lifts to $W(k)$ for a given k-bialgebra? We can guarantee that a bialgebra lifts uniquely by putting additional restrictions on n, r, and η. However, we also have unique liftings if the field k is the appropriate size. If a given bialgebra does not satisfy either of these conditions, we shall show that more than one lift to $W(k)$ exists.

Before explaining the restrictions, we shall describe in terms of Dieudonné modules what is necessary for a monogenic local–local bialgebra to lift uniquely. Let $H = \mathscr{H}(M)$, $M = E/E(F^n, F^r - \alpha^z V)$. Of course, we assume $r+1$ divides n or else H does not lift at all. By (2.1) all finite Honda systems are of the form (M, L_g) for some $g(F) \in (k[F]/(F^n))^\times$. In particular, we have L_1, the $W(k)$-module generated by $x = 1_M$. To show uniqueness of lifts, we simply need to show that all of the finite Honda systems are isomorphic, so $(M, L_1) \cong (M, L_g)$ for all $g(F)$. Recall that an isomorphism $\varphi : M \to M$ is given by an element $u(F) \in (k[F]/(F^n))^\times$. If we write $u(F) = \sum_{i=0}^{n-1} u_i F^i$ we get

$$u_i^{p^r} = \left(\frac{\eta}{\eta^{p^i}}\right) u_i^{p^{-1}}$$

for all i. In order for φ to be a morphism of finite Honda systems, we also have $\varphi(L_1) \subseteq L_g$. In other words:

Lemma 5.1. *Let $M = E/E(F^n, F^r - \alpha^z V)$, where $r+1$ divides n. Then $H = \mathscr{H}(M)$ lifts uniquely to $W(k)$ if and only if for all $g(F) \in (k[F]/(F^n))^\times$ there is a $u(F) = \sum_{i=0}^{n-1} u_i F^i, u_0 \ne 0$ and a $w \in W(k)$ such that*

(1) $u(F)x = wg(F)x$

(2) $u_i^{p^r} = (\alpha^z/\alpha^{zp^i})u_i^{p^{-1}}$, $0 \le i \le n-r-1$.

We shall refer to these conditions as conditions (1) and (2), respectively.

Remark. Note that, more generally, L_{g_1} and L_{g_2} give isomorphic lifts if and only if there is a $u \in k[F]$ and a $w \in W(k)$ so that

$$u(F)g_1(F)x = wg_2(F)x,$$
$$u_i^{p^r} = \left(\frac{\alpha^z}{\alpha^{zp^i}}\right) u_i^{p^{-1}}, \quad 0 \le i \le n-r-1.$$

We start by examining the size of k. Note that if $k = \mathbf{F}_p$ then E is a commutative ring, in which case

$$\alpha^z Vu(F)x = u(F)\alpha^z Vx = u(F)F^r x = F^r u(F)x$$

regardless of the choice of $u(F)$. It is not hard in this case to construct the necessary $u(F)$ and w once the question of $u(F)$ commuting with V and F^r is resolved. Thus if H is a monogenic $\mathbf{F}_p$-bialgebra, we can show it lifts uniquely. This result can be weakened somewhat.

Proposition 5.2. *Let $k = \mathbf{F}_{p^\ell}, k_0 = \mathbf{F}_{p^d}$ with $d = \gcd(\ell, r+1)$. Let $M = E/E(F^{s(r+1)}, F^r - \alpha^z V)$. Then $\mathscr{H}(M)$ lifts uniquely if $k \subseteq \mathbf{F}_{p^{r+1}}$ and $\alpha^z \in \mathbf{F}_p$.*

Proof. Let $w = 1$ and $u(F) = g(F)$. Condition (1) is clear, as is condition (2) since $g_i^{p^r} = g_i^{p^{-1}}$ and $\alpha^z = \alpha^{zp^i}$ for all i. □

We also have uniqueness of lifts if the size of the Dieudonné module (and hence the bialgebra) is sufficiently small.

Proposition 5.3. *Let $M = E/E(F^{r+1}, F^r - \alpha^z V)$. Then $\mathscr{H}(M)$ lifts uniquely.*

Proof. The trick here is that condition (2) only needs to hold for $i = 0$. Write $g(F) = \sum_{i=0}^{r} g_i F^i$. Let $u(F) = g_0^{-1} g(F)$ and $w = g_0^{-1}$. Condition (1) again is clear. Since the constant term of $u(F)$ is 1, condition (2) is immediate as well. □

Thus, any bialgebra whose Dieudonné module satisfies either the field condition or the size condition lifts uniquely. To complete Theorem 2, we need to show that if the bialgebra lifts uniquely then the corresponding Dieudonné module satisfies one of the two conditions. We shall do this with an example.

Example 5.4. For $\eta = \alpha^z \in k$, $\eta \notin \mathbf{F}_p$, let $g(F) = 1 + F$. Let $s = n/(r+1)$, $s > 1$. We shall show that (M, L_g) is not isomorphic to (M, L_1), thereby giving at least two lifts.

Let $w = \sum_{i=0}^{s-1} w_i p^i$. If there is an isomorphism given by a $u(F)$, then $u(F)x = wg(F)x$. We then have

$$u(F)x \equiv w_0 x + w_0 Fx (\mathrm{mod}\, F^{r+1}).$$

By condition (1) we have $w_0^{p^{r+1}} = w_0$ and $(w_0)^{p^r+1} = (\eta^p/\eta^{p^2})w_0$. Using the first equation, the second can be rewritten as

$$w_0 = \frac{\eta^p}{\eta^{p^2}} w_0$$

hence $\eta^p = \eta^{p^2}$, i.e. $\eta \in \mathbf{F}_p$, therefore no such $u(F)$ can exist. This proves the claim.

Of course, if $\eta = \alpha^z \in \mathbf{F}_p$, then $\alpha^{zp^{d-1}} = \alpha$, which is equivalent to saying z divides $(p^\ell - 1)/(p^d - 1)$.

6. The number of nonisomorphic lifts

Finally, we provide a formula for the number N of different isomorphism classes of lifts a monogenic k-bialgebra has to $W(k)$. Not surprisingly, the number will depend on the size of the field, the size of the Dieudonné module, as well as the value of z.

For the remainder of this paper, let $M = E/E(F^n, F^r - \alpha^z V)$ be a Dieudonné module that lifts. As $r+1$ divides n, set $s = n/(r+1)$. The construction of N will consist of calculating four other numbers:

1. N_g, the number of possible $g(F) \in (k[F]/(F^n))^\times$.
2. N_w, the number of invertible w's modulo p^n.
3. N_u, the number of automorphisms of M.
4. $N_{u,w}$, the number of automorphisms of W/p^nW that can generate new elements of $\mathrm{Aut}(M)$ in the sense described below.

For $u = u(F) \in \mathrm{Aut}(M)$ and $w \in W(k)$ clearly $(M, L_g) \cong (M, L_{ug})$ and $(M, L_g) \cong (M, L_{wg})$. The total number of nonisomorphic lifts is obtained by computing N_g and dividing by both N_u and N_w, and then multiplying by $N_{u,w}$ to eliminate double counting in the case where $ug = wg$. In other words

$$N = \frac{N_g N_{u,w}}{N_u N_w}$$

and it suffices to determine each of these constants.

1. N_g: We calculate the number of elements in $(k[F]/(F^n))^\times$, which is clearly $(p^\ell - 1)(p^\ell)^{n-1}$.
2. N_w: Since $p^s M = 0$ and $p^{s-1} M \neq 0$, for $w \in W$ to be counted it is of the form $\sum_{i=0}^{s-1} w_i p^i$ with $w_0 \neq 0$. Thus we obtain $N_w = (p^\ell - 1)(p^\ell)^{s-1}$.
3. N_u: We shall calculate $\mathrm{Aut}(M)$. First, we introduce the following function: for $0 \leq i \leq n-r-1$, define $f(z)$ to be the cardinality of $S = \{i \mid 1 \leq i \leq n-r-1, (p^d - 1) | (z(p^i - 1))\}$. S includes all multiples of d less than or equal to $n-r-1$. In fact, we have $(s-1)(r+1)/d \leq f(z) \leq n-r-1$. Equality on the left occurs when z and $p^d - 1$ are relatively prime (in which case the i's are only the multiples of d) and equality on the right when $z = 0$. Note that if $s = 1$, then we have $f(z) = 0$.

We are now in a position to compute the automorphism group.

Lemma 6.1. *Let* $M = E/E(F^n, F^r - \alpha^z V)$. *An element of* $\mathrm{Aut}(M)$ *is given by* $u(F) = \sum_{i=0}^{n-1} u_i F^i$ *where*

$$u_i \in \begin{cases} k_0^\times, & i = 0, \\ v_i k_0, & 1 \le i \le n-r-1,\ i \in S, \\ \{0\}, & 1 \le i \le n-r-1,\ i \notin S, \\ k, & n-r-1 \le i \le n-1, \end{cases}$$

where $v_i \in k$ satisfies $v_i^{p^{r+1}} = \alpha^{zp(1-p^i)} v_i$.

Proof. The coefficient u_0 is invertible and $u_i^{p^{r+1}} = \alpha^{zp(1-p^i)} u_i$ for all $0 \le i \le n-r-1$. When $i = 0$ we have $u_0^{p^{r+1}} = u_0$ hence $u_0 \in k_0^\times$.

Let $1 \le i \le n-r-1$. Let G be the multiplicative subgroup $\{x^{p^d-1} \mid x \in k^\times\} \subset k^\times$. If $u_i^{p^{r+1}} = \alpha^{zp - zp^{i+1}} u_i$, $u_i \ne 0$, then $u_i^{p^{r+1}-1} \in G$, so we have

$$\alpha^{zp^{i+1} - zp} \in G.$$

Since G consists of all $\alpha^{j(p^d-1)}$ let $zp^{i+1} - zp = pz(p^i - 1)$ be some multiple of $p^d - 1$. Since p and $p^d - 1$ are coprime, then a nontrivial u_i exists if and only if $p^d - 1$ divides $z(p^i - 1)$, i.e. if and only if $i \in S$. Furthermore, if v_i satisfies the above condition, then so does av_i for all $a \in k_0$. As these are the only solutions, it is clear that there are $|k_0| = p^d$ different choices for u_i when $i \in S$, and the single choice 0 for $i \notin S$.

Of course, for $n - r \le i \le n$ there are no restrictions, hence $u_i \in k$, and the lemma is proved. □

We can now quickly calculate $N_u = (p^d - 1)(p^d)^{f(z)}(p^\ell)^r$.

4. $N_{u,w}$: The issue here is to determine when $u(F)g = wg$ to eliminate any double counting that might have occurred. We shall rephrase this as follows: given $u(F)$, how many invertible $w \in W(k)$ are there such that multiplication by $w^{-1}u(F)$ is an automorphism? Write $w^{-1} = \sum_{i=0}^{s-1} v_i p^i$ and $u(F) = \sum_{j=0}^{n-1} u_j F^j$.
   Again let $\eta = \alpha^z w^{-1} u(F)$ be written as

$$\sum_{i=0}^{s-1} v_i p^i \sum_{j=0}^{n-1} u_i F^i = \sum_{i=0}^{s-1} \sum_{j=0}^{n-1} u_j v_i F^{i(r+1)+j}.$$

   Clearly, the constant term $u_0 v_0$ is invertible, so for $w^{-1}u(F)$ to be an automorphism we need only satisfy

$$(u_j v_i)^{p^r} = \frac{\eta}{\eta^{p^{i(r+1)+j}}} u_j v_i, \quad i(r+1) + j \le n-r-1 = (s-1)(r-1).$$

Since $u_j^{p^r} = \eta^{1-p^j} u_j$ this condition reduces to

$$v_i^{p^r} = \frac{\eta}{\eta^{p^{i(r+1)}}} v_i.$$

The solutions of this equation are all of the form

$$v_i = a\eta^{-\frac{p(p^{i(r+1)}-1)}{p^{r+1}-1}}, \quad a \in k_0$$

and since $v_0 \neq 0$ we have $N_{u,v} = (p^d - 1)(p^d)^{s-1}$.

Finally, we compute N:

$$N = \frac{N_g N_{u,w}}{N_u N_w} = \frac{(p^\ell - 1)(p^\ell)^{n-1}(p^d - 1)(p^d)^{s-1}}{(p^d - 1)(p^d)^{f(z)}(p^\ell)^r(p^\ell - 1)(p^\ell)^{s-1}}$$

$$= (p^\ell)^{r(s-1)}(p^d)^{s-1-f(z)}$$

and the third theorem is proved.

Remark. Of course, the uniqueness questions of Section 5 follow directly from this formula. If $s = 1$ then $f(z) = 0$ and N is clearly equal to 1. If $k \subseteq \mathbf{F}_{p^{r+1}}$ and $\alpha^z \in \mathbf{F}_p$ then $d = \ell$ and $(p^\ell - 1)/(p - 1)$ divides z. Write $z = z_0((p^\ell - 1)/(p - 1))$. For any $1 \leq i \leq n - r - 1$ we have

$$z(p^i - 1) = z_0(p^\ell - 1)\frac{p^i - 1}{p - 1} = \left(z_0 \frac{p^i - 1}{p - 1}\right)(p^d - 1),$$

hence $f(z) = n - r - 1$ and $N = 1$.

It is possible at this point to construct a formula for the number of isomorphism classes of monogenic bialgebras over $W(k)$ of rank p^n which are local–local mod p, which is derived by combining Theorem 3 with Corollary 3.2. However, the formula

$$\sum_{\{r:r+1|n\}} \sum_{z=0}^{p^{\gcd(\ell, r+1)}-2} p^{\ell(n-r-1)+\gcd(\ell,r+1)((n/r+1)-1-f(z))}$$

is perhaps too complicated to be useful in general, even for small n.

References

[1] L. Childs, K. Zimmerman, Congruence–torsion subgroups of dimension one formal groups, J. Algebra 170 (1994) 929–955.
[2] J.M. Fontaine, Groupes finis commutatifs sur les vecteurs de Witt, C. R. Acad. Sci. Paris 280 (1975) 1423–1425.
[3] A. Grothendieck, Groupes de Barsotti-Tate et Cristaux de Dieudonné, Les Presses de L'Université de Montreal, Canada, 1974.
[4] N. Jacobson, Lectures in Abstract Algebra III – Theory of Fields and Galois Theory, Springer, New York, 1964.
[5] A. Koch, Lifting Witt subgroups to characteristic zero, New York J. Math. 4 (1998) 127–136.
[6] A. Koch, Cyclic Dieudonné modules and Witt subgroups killed by p, Rocky Mountain J. Math., to appear.

[7] F. Oort, D. Mumford, Deformations and lifings of finite, commutative group schemes, Invent. Math. 5 (1968) 317–334.
[8] J. Roubaud, Schémas en groupes finis sur un anneau de valuation discrèt et systèmes de Honda associés, Université de Paris-Sud, Paris, 1992.
[9] J. Tate, F. Oort, Group schemes of prime power order, Ann. Sci. Ecole Norm. Sup. 3 (1970) 1–21.
[10] W. Waterhouse, Introduction to Affine Group Schemes, Springer, New York, 1979.